PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-130098
(43)Date of publication of application : 25.05.1993

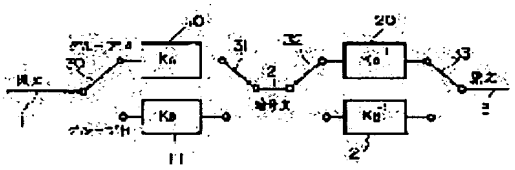
(51)Int.CI. H04L 9/06
H04L 9/14
G06F 15/30
G06K 17/00
G09C 1/00
H04K 1/00

(21)Application number : 03-286348
(22)Date of filing : 31.10.1991

(71)Applicant : HITACHI LTD
(72)Inventor : KANEKAWA NOBUYASU

(54) TRANSMISSION METHOD FOR CIPHERING DATA AND CARD WITH CIPHERING DATA RECORDED THEREON

(57)Abstract:
PURPOSE: To preclude the possibility of ciphering from being decoded by a third party by using plural ciphering systems or ciphering keys depending on types of characters, codes and data used for an original text.
CONSTITUTION: Codes, characters and data with high frequency of appearance of an original text are classified into a group A and codes characters and data with low frequency of appearance are classified into a group B. The codes characters and data classified into the group A are ciphered by a ciphering operation 10 employing the ciphering system or ciphering key KA corresponding to the group A and the codes characters and data classified into the group B are ciphered by a ciphering operation 11 employing the ciphering system or ciphering key KB corresponding to the group B and a ciphered text 2 is obtained. The ciphered text 2 is sent from a sender side to a receiver side through various transmission means. A ciphering decoding operation 20 (21) corresponding to each group at the receiver side is used to decode the ciphered text thereby obtaining an original text 3.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－130098

(43)公開日　平成５年(1993)５月25日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ	9/06				
	9/14				
Ｇ０６Ｆ	15/30	３４０	6798－5L		
Ｇ０６Ｋ	17/00		L 8623－5L		
			7117－5K	Ｈ０４Ｌ　9/ 02	Ｚ

審査請求　未請求　請求項の数20(全 13 頁)　最終頁に続く

(21)出願番号　特願平3－286348

(22)出願日　平成３年(1991)10月31日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　金川　信康
茨城県日立市久慈町4026番地　株式会社日立製作所日立研究所内

(74)代理人　弁理士　鵜沼　辰之

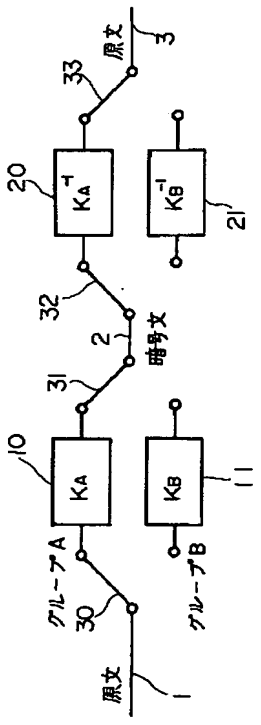
(54)【発明の名称】　暗号化データの伝送方法及び暗号化データが記録されたカード

(57)【要約】

【目的】　リモートセンシングデータ、有料の放送内容、コンピュータデータ、ＩＤカードなどの特定の符号パターンの出現頻度が極端に高く、原文のパターンが容易に推定されやすく、暗号が解読されやすい用途での暗号化データの伝送方法を提供すること。

【構成】　原文において、出現頻度が高いパターン（符号）のグループと低いパターン（符号）グループとに分類し、それぞれのグループごとに別々の暗号化方式または、暗号化鍵を用いて暗号化する。

【効果】　本発明によれば、原文中の符号の出現頻度に関する知識や、原文の推定を手がかりにして、暗号が第三者に解読される畏れを少なくすることができる。



1

【特許請求の範囲】

【請求項１】　原文のデータを暗号化して伝送するデータ伝送方法であって、原文を構成する文字、符号、データの種別に応じて複数の暗号化方式または、暗号化鍵を使いわけることを特徴とする暗号化データの伝送方法。

【請求項２】　原文のデータを暗号化して伝送する暗号化データの伝送方法であって、暗号化データの送信側で原文において出現頻度が高いパターンが属するグループと出現頻度の低いパターン（符号）が属するグループとに分類し、それぞれのグループ毎に異なる暗号化方式または、暗号化鍵で原文を暗号化することを特徴とする暗号化データの伝送方法。

【請求項３】　ＤＰＣＭ方式でデータ圧縮を行ってデータ伝送を行う際に、ＤＰＣＭ方式の差分０を表す符号と差分０以外を表す符号とでは別個の暗号化方式または暗号化鍵を使用して暗号化することを特徴とする請求項１に記載の暗号化データの伝送方法。

【請求項４】　加入放送におけるテストパターンの映像信号と通常の放送番組の映像信号とでは別個の暗号化方式または暗号化鍵を使用して暗号化することを特徴とする請求項１に記載の暗号化データの伝送方法。

【請求項５】　コンピュータデータのうち＄ＦＦ、＄００、またはＮＯＰを表す機械語に相当するデータとそれ以外のデータとでは別個の暗号化方式または暗号化鍵を使用して暗号化することを特徴とする請求項１に記載の暗号化データの伝送方法。

【請求項６】　キャッシュカードに各種データを記録し、記録された前記各種データを読み取るデータ伝送方法であって、キャッシュカードの口座番号と暗証番号とでは別個の暗号化方式または暗号化鍵を使用して暗号化することを特徴とする請求項１に記載の暗号化データの伝送方法。

【請求項７】　ＩＤカードを用いてＩＤカードに記録されたデータを送信する際にＩＤ番号と暗証番号とでは別個の暗号化方式または暗号化鍵を使用して暗号化してＩＤカードに記録することを特徴とする請求項１に記載の暗号化データの伝送方法。

【請求項８】　ＤＰＣＭ方式でデータ圧縮を行ってデータ伝送を行う際に、出現頻度が高いパターン（符号）のグループがＤＰＣＭ方式の差分０を表す符号から構成され、出現頻度が低いパターン（符号）のグループがＤＰＣＭ方式の差分０以外を表す符号から構成されることを特徴とする請求項２に記載の暗号化データの伝送方法。

【請求項９】　加入放送におけるデータ伝送であって、出現頻度が高いパターン（符号）のグループが加入放送におけるテストパターンの映像信号から構成され、出現頻度が低いパターン（符号）グループが通常の放送番組の映像信号から構成されていることを特徴とする請求項２に記載の暗号化データの伝送方法。

【請求項１０】　コンピュータデータを伝送する際に、

2

出現頻度が高いパターン（符号）のグループがコンピュータデータのうち＄ＦＦ、＄００、またはＮＯＰを表す機械語から構成され、出現頻度が低いパターン（符号）グループがそれ以外のデータから構成されていることを特徴とする請求項２に記載の暗号化データの伝送方法。

【請求項１１】　キャッシュカードに各種データを記録し、記録された前記各種データを読み取るデータ伝送方法であって、出現頻度が高いパターン（符号）のグループがキャッシュカードの口座番号から構成され、出現頻度が低いパターン（符号）のグループが暗証番号から構成されていることを特徴とする請求項２に記載の暗号化データの伝送方法。

【請求項１２】　出現頻度が高いパターン（符号）のグループがＩＤカードのＩＤ番号から構成され、出現頻度が低いパターン（符号）のグループが暗証番号から構成されていることを特徴とする請求項２に記載の暗号化データの伝送方法。

【請求項１３】　原文を暗号化して伝送する暗号化データの伝送方法であって、原文において出現頻度が高いパターンが属する第１のグループと、出現頻度が低いパターンが属する第２のグループとに分類し、これら各グループに対して相互に異なる暗号化方式または暗号化鍵を割り当てると共に、第１、第２のグループについて相互に異なる暗号化方式または暗号化鍵で暗号化された際に第２のグループに属する暗号文のパターンが第１のグループの暗号文のパターンと同一になる第２のグループの原文のパターンに対して第１、第２のグループとは異なる暗号化方式または暗号化鍵を割り当てて原文を暗号化することを特徴とする請求項２に記載の暗号化データの伝送方法。

【請求項１４】　暗号化されたデータを伝送する暗号化データ伝送システムにおいて、原文と原文のうち出現頻度の高い第１のグループに属するパターン群とを比較し、一致するか否かを判定する第１の比較器群と、

前記原文と原文のうち出現頻度の低い第２のグループに属するパターン群とを比較し、一致するか否かを判定する第２の比較器群と、

前記第１の比較器群の出力信号の論理和をとる第１の論理和演算手段と、

前記第２の比較器群の出力信号の論理和をとる第２の論理和演算手段と、

前記第１、第２の論理和演算手段の出力信号を取り込み負論理の論理積をとる論理積演算手段とを有し、前記第１、第２の論理和演算手段及び論理積演算手段の出力信号に基づいて前記原文のパターンをグループ分けすることを特徴とする暗号化データ伝送システムのグループ判別装置。

【請求項１５】　暗号化されたデータを伝送する暗号化データ伝送システムにおいて、

原文の出現頻度に応じて所定の暗号化方式または暗号化

鍵を用いて暗号化された暗号文と原文において出現頻度の高い第１のグループに属する原文のパターン群に対応する暗号文のパターン群とを比較し一致するか否かを判定する第１の比較器群と、
前記暗号文と原文において出現頻度の低い第２のグループに属する原文のパターン群に対応する暗号文のパターン群とを比較し、一致するか否かを判定する第２の比較器群と、
前記第１の比較器群の出力信号の論理和をとる第１の論理和演算手段と、
前記第２の比較器群の出力信号の論理和をとる第２の論理和演算手段と、
前記第１、第２の論理和演算手段の出力信号を取り込み負論理の論理積をとる論理積演算手段とを有し、前記第１、第２の論理和演算手段及び論理積演算手段の出力信号に基づいて前記暗号文のパターンを原文に対応してグループ分けすることを特徴とする暗号化データ伝送システムのグループ判別装置。

【請求項１６】　ＤＰＣＭ方式でデータ圧縮を行ってデータを伝送する圧縮化データの伝送方法であって、ＤＰＣＭ方式の差分０を表す符号と差分０以外を表す符号とでは別個の暗号化方式または暗号化鍵を使用して暗号化することを特徴とする圧縮化データの伝送方法。

【請求項１７】　加入放送におけるテストパターンの映像信号と通常の放送番組の映像信号とでは別個の暗号化方式または暗号化鍵を使用してスクランブリングすることを特徴とする加入放送番組のスクランブリング方法。

【請求項１８】　コンピュータデータのうち＄ＦＦ、＄００、またはＮＯＰを表す機械語に相当するデータとそれ以外のデータとでは別個の暗号化方式または暗号化鍵を使用して暗号化することを特徴とするコンピュータデータの伝送方法。

【請求項１９】　キャッシュカードの口座番号と暗証番号とでは別個の暗号化方式または暗号化鍵を使用して暗号化して記録されまたは、別個の記録方式を用いて記録されたことを特徴とするキャッシュカード。

【請求項２０】　ＩＤカードのＩＤ番号と暗証番号とでは別個の暗号化方式または暗号化鍵を使用して暗号化して記録されまたは、別個の記録方式を用いて記録されたことを特徴とするＩＤカード。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、暗号化されたデータの伝送の方法に係り、特に解読されにくい（暗号強度の高い）暗号化データの伝送方法及び暗号化データが記録されたカードに関する。

【０００２】

【従来の技術】従来から通信の秘密を確保するために、通信文を暗号化して伝送することが行なわれてきた。とくに近年では、コンピュータシステムの普及に伴う情報

化が進み、コンピュータ間を結ぶネットワークや、通信路での情報の漏洩が問題となる。

【０００３】文献（松井 甲子雄著「コンピュータのための暗号組立法入門、森北出版株式会社（１９８６）によると暗号化の方法には大きく分けて、原文の文字系列の順序を入れ替える「転置式暗号」、原文の文字を他の文字に置き換える「換字式暗号」に分けられる。また、暗号の強度を増すために、これらを組み合わせる「混合式暗号」が広く用いられている。

【０００４】「混合式暗号」のうち米国で標準化された暗号化規格の一つに「ＤＥＳ（Data Encryption Standard）暗号」がある。この方法は、上記文献ｐｐ．９４－１０５に示すように６４ビットを１ブロックとしたデータを１６段にわたって転置と換字を繰り返すものである。

【０００５】また原文中の文字の出現度数の分布が暗号解読の手掛かりとなるのを防ぐために、原文中の文字の出現度数分布を隠匿する「隠匿度数暗号」と呼ばれるものもある。この方法は、出現頻度の高い文字を出現頻度に合わせて複数の暗号文の文字に変換する方式で、原文の文字の出現頻度が暗号文の文字の出現頻度に反映しない特徴がある。

【０００６】

【発明が解決しようとする課題】従来から用いられていた「ＤＥＳ暗号」は、６４ビットを１ブロックとして処理をするために、原文がブロック単位で同一のパターンである場合には暗号文もブロック単位で同一のパターンとなる。従って以下に示すような用途に用いる場合は、原文と暗号文のブロックごとの出現度数の関連から暗号解読の手掛かりを第三者に与えるおそれがある。

【０００７】また、「ＤＥＳ暗号」に代表される混合式暗号は、複数の暗号化手段を組み合わせても原文の出現頻度が暗号文の出現頻度に伝搬する短所がある。

【０００８】従来から用いられている「隠匿度数暗号」は、原文の文字の出現頻度が暗号文の文字の出現頻度に反映しないように考慮した暗号化方式で、原文の内容の推定を困難にすることにより、第三者に暗号解読の手掛かりを与えないようにしている。この方法は、人間が日常読み書きする文書を暗号化するのには十分な暗号強度をもっている。しかし、近年急激に普及したコンピュータなどへの使用について、十分な考慮がされていなかった。

【０００９】暗号の隠匿性を守るためには、暗号化の方式すなわち「鍵」の隠匿性の保護はもとより、原文の内容の隠匿性も必要である。原文の内容が容易に推定可能な場合には、第三者に暗号解読の手がかりを与えることになる。以下に示すような用途では、原文の内容が容易に推定されやすい。

【００１０】遠隔地での計測値を伝送するリモートセンシングでは、通常データの差分をとりだしてデータを圧

縮して伝送する際にデータの差分のみを伝送するＤＰＣＭ（Differential Pulse Code Modulation）方式と呼ばれる方法がとられる。この場合、差分０を表す符号の出現頻度が極めて高い。

【００１１】有料の衛星放送などの加入放送では、加入者以外には放送番組が視聴できないように放送内容を暗号化（スクランブリング）し、加入者のみにスクランブリングした信号を解読するデコーダを配布することが多い。しかし、通常放送だけでなく、テストパターンまでスクランブリングして送出すると、テストパターンの規則性からスクランブリングされた信号解読の手がかりを第三者に与えることになる。

【００１２】コンピュータで扱うデータには、いわゆる人間が日常読み書きする文書の他に、プログラムや数値データなどの多様なデータが含まれている。

【００１３】これらのうち機械語によるプログラムには、＄００や＄ＦＦ（＄は１６進数を示す。）、そしてＮＯＰ（Non Operation）命令に相当する符号が極めて高い頻度で出現する。これらの出現頻度は、人間が日常読み書きする英語の文書で最も出現頻度の高いとされている文字“Ｅ”の出現頻度とは比較にならないほどである。

【００１４】仮りに＄００や＄ＦＦの符号が他の符号の１０倍の出現頻度をもつとすると、出現頻度を隠匿するためにはそれぞれに１０種類の暗号の符号を割り当てなければならない。このように出現頻度の高い１つの原文の符号に複数の暗号文の符号を割り当てるためには、本例のように原文の符号の数と暗号文の符号の数とが２５６個と同数である場合には、逆に出現頻度の低い複数の原文の符号に１つの暗号文の符号を割り当てなければならない。従って暗号を解読するに当って、暗号文に対して一義的に原文が対応しない。このことは、機械的に暗号を解読するコンピュータにおいては大きな問題となる。

【００１５】また、ＩＤカードや、キャッシュカードなどでは、カードの磁気記録部分にＩＤカードにおいてはＩＤ番号、キャッシュカードにおいては口座番号が、暗証番号とともに記録されている。これらのカードは、通常、ＩＤ番号、口座番号はカード表面に記入されている場合が多い。従って、磁気記録部分が暗号化されている場合には、原文であるＩＤ番号、口座番号とそれらに対応する磁気記録部分の暗号文を比較することにより暗号化方式を推定することができる。従って、暗証番号に相当する原文を第三者に解読されてしまう畏れがある。また、磁気記録部分が暗号化されておらず、公開されているコード体系、記録方式を用いている場合でも、ＩＤ番号、口座番号とそれらに対応する磁気記録部分を比較することによりどのコード体系、記録方式を使用しているかが第三者にわかってしまい、暗証番号を読みだすための手掛かりを与えてしまう。

【００１６】リモートセンシングデータ、有料の放送内容、コンピュータデータ、ＩＤカードなどにおいて特定の符号パターンの出現頻度が極端に高く、原文のパターンが容易に推定されやすく、暗号が解読されやすい用途での暗号化によるデータ伝送方式を提供することを目的とする。

【００１７】

【課題を解決するための手段】上記目的を達成するために本発明では、伝送すべきデータの暗号化は以下のように行われる。

【００１８】原文において、出現頻度が高いパターン（符号）のグループと出現頻度が低いパターン（符号）のグループとに分類し、それぞれのグループごとに別々の暗号化方式または、暗号化鍵を用いて暗号化する。

【００１９】ＤＰＣＭ方式のリモートセンシングデータの伝送においては、差分０を表す符号と差分０以外を表す符号とを別々の暗号化方式または、暗号化鍵を用いて暗号化する。

【００２０】有料の衛星放送などの加入放送では、テストパターンの画像と通常の放送番組とで別々の暗号化方式または、暗号化鍵を用いて暗号化（スクランブリング）する。

【００２１】コンピュータで扱うデータの伝送においては出現頻度の高い＄００や＄ＦＦ、そしてＮＯＰ（Non Operation）命令に相当する符号と、それ以外の符号とを別々の暗号化方式または、暗号化鍵を用いて暗号化する。

【００２２】ＩＤカードや、キャッシュカードなどにおいては、ＩＤ番号、口座番号と暗証番号とを別々の暗号化方式または暗号化鍵を用いて暗号化する。

【００２３】

【作用】本発明によれば、原文において、出現頻度が高いパターン（符号）のグループと低いパターン（符号）グループとに分類しているために、それぞれのグループ毎に別々の暗号化方式または、暗号化鍵を用いて暗号化するため、出現頻度が高いパターン（符号）のグループが手がかりになって、出現頻度が低いパターン（符号）グループの暗号が解読されることがない。

【００２４】またＤＰＣＭ方式のリモートセンシングデータの伝送においては、差分０以外のデータが重要であり、本発明によれば差分０を表すデータの出現頻度が高いという事前の知識から、差分０以外を表すデータに相当する暗号文を第三者に解読される畏れが少なくなる。

【００２５】一方、有料の衛星放送では、テストパターンの画像の持つ規則性から、通常の放送番組のスクランブリングを第三者に解読される畏れが少なくなる。

【００２６】またコンピュータで扱うデータの伝送においては、原文中の＄００や＄ＦＦ、そしてＮＯＰ命令に相当する符号の出現頻度が高いという知識からそれ以外の符号に相当する暗号文が第三者に解読される畏れが少

なくなる。

【００２７】更にＩＤカードや、キャッシュカードなどにおいては、カードに記載されているＩＤ番号、口座番号を手掛かりに暗証番号に相当する暗号が第三者に解読される畏れが少なくなる。

【００２８】

【実施例】以下、本発明の実施例を図面を参照して説明する。

【００２９】図１には本発明に係る暗号化データの伝送方法の原理が示されている。同図において原文１の符号、文字、データは出現頻度に応じて、出現頻度の高い符号、文字、データはグループＡに、出現頻度の低い符号、文字、データはグループＢに分類される。グループＡに分類された符号、文字、データはグループＡに対応したＫＡなる暗号化方式または、暗号化鍵を用いる暗号化操作１０により暗号化され、グループＢに分類された符号、文字、データはグループＢに対応したＫＢなる暗号化方式または、暗号化鍵を用いる暗号化操作１１により暗号化され暗号文２が得られる。この暗号文２が送信側から受信側へ種々の伝送手段により送信される。

【００３０】一方、暗号文の受信側では、それぞれのグループに対応した暗号解読操作２０，２１で暗号を解読し、原文３を得ることができる。出現頻度が高い符号、文字、データの集合体であるグループＡの暗号は解読されやすい。しかし、本実施例によれば、グループＢの暗号はグループＡとは別個の暗号化方式、または暗号化鍵を用いているので解読されにくい。

【００３１】また極端な場合、グループＡの原文の内容は第三者に知られても構わない場合には、グループＡの原文は暗号化せず、グループＢの原文のみ暗号化することも有効である。

【００３２】図２、図３には、本発明に係る暗号化データの伝送方法における原文のグループ判別の方式が示されている。図２に示すようにグループＡに属する原文はＫＡなる暗号化方式または、暗号化鍵を用いる暗号化操作１０により暗号化され、グループＢに属する原文はＫＢなる暗号化方式または、暗号化鍵を用いる暗号化操作＊１１により暗号化される。

＊

$$C = K \text{ eor } x$$

但し、Ｃ：暗号
Ｋ：暗号化鍵
ｘ：原文
eor：排他的論理和演算子

※

$$Ca = KA \text{ eor } xa$$
$$Cb = KB \text{ eor } xb$$

サブグループａ，ｂに属する原文ｘａ，ｘｂは暗号化鍵★

★

$$KA \text{ eor } xa = KB \text{ eor } xb$$
$$\therefore xb = KB \text{ eor } KA \text{ eor } xa$$

である。ここで、サブグループｂに属する原文ｘｂは暗☆

☆

$$Cb' = KX \text{ eor } xb$$

ここで、Ｃｂ′が他の暗号化鍵による暗号と識別が可能であるためには、

【００３３】上記のように暗号化するとグループＢのうちサブグループｂとグループＡのうちサブグループａが同じ暗号文に暗号化される場合がある。すると、暗号の受信側では、暗号文の符号がグループＡに属するものなのかグループＢに属するものなのか判別できない。コンピュータを用いて暗号化、暗号解読を行う場合には、ヒューリスティックス（直感的知識）を使用できないために、暗号文と原文とは一義的に対応しなければならない。このような場合には、図３に示すようにグループ判別手段４０の結果４１を暗号の受信側にも送ればよい。図３において、グループ判別結果４１に基づきスイッチ３０，３１，３２，３３を切り替えてグループごとに適した暗号化方式または、暗号化鍵を選択して暗号化及び、暗号解読を行う。

【００３４】図４にはグループ判別手段４０の具体的構成が示されている。同図においてグループＡに属するパターン群４２－１～４２－Ｎと原文１のパターンとが比較手段４３－１～４３－Ｎで比較され、原文１がグループＡに属するパターン群４２－１～４２－Ｎのいずれかと一致した場合には原文１のパターンがグループＡに属すると判定され、オアゲート４４を介して判別結果４１が出力される。

【００３５】次に図５、図６に図２、図３に示す実施例においてグループ判定結果４１を暗号の送信側から受信側へ送る必要をなくした実施例を示す。これらの図において暗号化方式または、暗号化鍵ＫＢを用いる暗号化操作１１によってサブグループａと同じ暗号に暗号化されるサブグループｂをＫＢとは異なる暗号化方式または、暗号化鍵ＫＸを用いる暗号化操作１２で暗号化することによってサブグループａと同じ暗号に暗号化されることを防止している。

【００３６】暗号化方式または、暗号化鍵ＫＸの定め方は、暗号化方式または、暗号化鍵ＫＡ，ＫＢによって異なる。たとえば式（１）のように排他的論理和（exclusive-or）により暗号化する場合を考える

……（１）

※図２においてサブグループａ，ｂに属する原文ｘａ，ｘｂは暗号化鍵ＫＡ，ＫＢにより以下のように暗号Ｃａ，Ｃｂに変換される。

【００３７】

……（２）
……（３）

★ＫＡ，ＫＢにより同一の暗号に変換されるから、

……（４）
……（４′）

☆号化鍵ＫＸにより暗号Ｃｂ′に暗号化されるから、

……（５）

Ｃｂ′ ！∈ {ＣＡ：ＣＡ＝ＫＡ eor ｘＡ} かつ、
Ｃｂ′ ！∈ {ＣＢ：ＣＢ＝ＫＢ eor ｘＢ}　　……（６）
となるように暗号化鍵ＫＸを選べばよい。ここでｘＡは＊を表している。グループＡに属する原文、ｘＢはグループＢに属する原文であり、！∈は∈の否定、すなわち「属さない」こと＊

ＫＸ＝ＫＡ　　……（７）
とおくと、
Ｃｂ′ ＝ＫＡ eor ｘｂ ！∈ {ＣＡ：ＣＡ＝ＫＡ eor ｘＡ}
また、ＫＡ eor ＫＡ＝０であるから、式（４′）より
Ｃｂ′ ＝ＫＢ eor ｘｂ ！∈ {ＣＢ：ＣＢ＝ＫＢ eor ｘＢ}
となり、暗号化鍵ＫＸは式（６）の条件を満たすことができる。

【００３９】次に図７を参照して具体的なデータを例にして説明する。同図において、＄ＦＦ（２進数で 1111 1111）、＄００（２進数で 0000 0000）をグループＡに属す原文と仮定し、それ以外のデータをグループＢとする。また、暗号化鍵ＫＡ，ＫＢをそれぞれ＄ＡＡ（２進数で 1010 1010）、＄９９（２進数で 1001 1001）と仮定する。

【００４０】グループＡに属す原文＄ＦＦ、＄００は暗号化鍵ＫＡとのビットごとの排他的論理和演算によって図７に示すように暗号＄ＡＡ（２進数で 1010 1010）、＄５５（２進数で 0101 0101）に変換される。

【００４１】一方、暗号化鍵ＫＢによって暗号＄ＡＡ、＄５５に変換される符号すなわちサブグループｂに属する符号は、それぞれ＄３３（２進数で 0011 0011）、＄ＣＣ（２進数で 1100 1100）である。従ってサブグループｂに属する符号＄３３、＄ＣＣは暗号化鍵ＫＡによってそれぞれ暗号＄６６（２進数で 0110 0110）、＄９９（２進数で 1001 1001）に変換される。

【００４２】暗号の受信側では、暗号＄ＡＡ、＄５５、＄６６、＄９９が来たら、暗号化鍵ＫＡを用いて暗号を解読し、それ以外の暗号が来たら暗号化鍵ＫＢ用いて暗号を解読すれば、原文を得ることができる。

【００４３】本実施例によれば、グループ判別結果を受信側に送る必要がなくなるので、伝送する情報量が少なくてすむほか、第３者に暗号解読のヒントを与える機会も少なくなる。

【００４４】図８には、図５、図６に示した実施例における暗号化鍵ＫＡ，ＫＢが固定パターン（時系列的に変化しないパターン）である場合のグループ判別手段４０Ａの具体的構成が示されている。暗号化鍵が固定パターンである場合には、グループＡに属するパターン群４２－１～４２－Ｎが判れば、サブグループｂに属するパターン群４４－１～４４－Ｎも固定パターンとして予め決定できるため、以下のように原文１と固定パターンとを比較することにより原文のグループ判別が可能となる。

【００４５】まずグループＡに属するパターン群４２－１～４２－Ｎと原文１のパターンとが比較手段４３－１～４３－Ｎで比較され、原文１がグループＡに属するパターン群４２－１～４２－Ｎのいずれかと一致した場合には原文１のパターンがグループＡに属する判定され、オアゲート５０－１を介して判別結果４１（４１Ａ）が出力される。

【００４６】次にサブグループｂに属するパターン群４４－１～４４－Ｎと原文１のパターンとが比較器群４５－１～４５－Ｎで比較され、原文１がサブグループｂに属するパターン群４４－１～４４－Ｎのいずれかと一致した場合には原文１のパターンがサブグループｂに属すると判定され、オアゲート５０－２を介して判別結果４１（４１Ｂ）が出力される。

【００４７】また、上記（１）にも（２）にも該当しない場合には原文１のパターンがサブグループｂを含まないグループＢに属すると判定され、オアゲート５０－２、アンドゲート５１を介して判別結果４１（４１ｃ）が出力される。

【００４８】図９は、図５、図６に示した実施例における暗号化鍵ＫＡ，ＫＢが固定パターンである場合のグループ判別手段４０Ｂの実施例である。この場合もグループＡに属する暗号のパターン群４６－１～４６－Ｎが判れば、サブグループｂに属する暗号のパターン群４８－１～４８－Ｎも固定パターンとして予め決定できるため、以下のように原文１の暗号文２と固定パターンとを比較することにより暗号文のグループ判別が可能となる。

【００４９】まずグループＡに属する暗号のパターン群４６－１～４６－Ｎと暗号文２のパターンとが比較手段４７－１～４７－Ｎで比較され、暗号文２がグループＡに属する暗号のパターン群４６－１～４６－Ｎのいずれかと一致した場合には暗号文２のパターンがグループＡに属する暗号と判定され、オアゲート６０－１を介して判別結果６２（６２Ａ）が出力される。

【００５０】次にサブグループｂに属する暗号のパターン部４８－１～４８－Ｎと暗号文２のパターンとが比較手段４９－１～４９－Ｎで比較され、暗号文２がサブグループｂに属する暗号のパターン群４８－１～４８－Ｎのいずれかと一致した場合には暗号文２のパターンがサブグループｂに属する暗号と判定され、オアゲート６０－２を介して判別結果６２（６２Ｂ）が出力される。

【００５１】また、暗号文２がパターン群４６－１～４

６－Ｎ、あるいはパターン群４８－１～４８－Ｎのいずれにも一致しない場合にはオアゲート６０－１，６０－２及びアンドゲート６１により暗号文２のパターンがサブグループｂの暗号を含まないグループＢに属すると判定され、判別結果６２（６２Ｃ）が出力される。

【００５２】また、暗号化鍵ＫＡ，ＫＢが固定パターンでなく、シフトレジスタなどを用いて生成されたＭ系列などの乱数である場合には、サブグループｂに属するパターン群４４－１～４４－Ｎは、図１０に示すようにグループＡに属するパターン群４２－１～４２－Ｎ及び、暗号化鍵ＫＡ，ＫＢによって決定される。

【００５３】この場合、サブグループｂに属する暗号のパターン群４８－１～４８－Ｎは、図１１に示すようにサブグループ（ｂ）に属するパターン群４４－１～４４－Ｎ及び、暗号化鍵ＫＸによって決定される。

【００５４】なお以下に示す実施例では、簡単のために図２、図３に示した実施例の応用例について説明を加えるが、図５，図６に示した実施例も適用可能であることは勿論のことである。

【００５５】図１２，図１３には遠隔地の計測点１００での計測データをＤＰＣＭ方式により圧縮して遠隔地の処理センタ１０１へ伝送する暗号化データ伝送方式の実施例が示されている。図１３に示すように差分０に相当する符号をＫＡなる暗号化方式または、暗号化鍵を用いた暗号化操作１０により暗号化し、差分０以外の値に相当する符号をＫＢなる暗号化方式または、暗号化鍵を用いた暗号化操作１１により暗号化して、暗号文２を得る。得られた暗号文２は公衆通信回線などの種々の伝送手段により受信側に伝送される。暗号文の受信側では、それぞれのグループに対応した暗号解読操作２０，２１で暗号を解読し、原文を得ることができる。

【００５６】本実施例によれば、差分０のＤＰＣＭ符号の出現頻度が高いという知識から差分０以外の値を表すＤＰＣＭ符号の解読の手掛かりを第三者に与える畏れがなくなる。

【００５７】次に図１４、図１５に本発明を加入放送のスクランブリングに適用した実施例を示す。これらの図において放送事業者１０２では、加入者以外が放送を聴取するのを防ぐために、放送内容を暗号化（スクランブリング）して、無線又は有線により加入者１０３へ放送内容を送る。加入者１０３では、放送事業者より配布されたデコーダにより暗号（スクランブリング）を解読して放送を聴取することができる。本実施例では、図１５に示すようにテストパターンをＫＡなる暗号化方式または、暗号化鍵による暗号化操作１０により暗号化（スクランブリング）し、通常の放送をＫＢなる暗号化方式または、暗号化鍵による暗号化操作１１により暗号化（スクランブリング）して、暗号文２を得る。得られた暗号文２は無線や有線などの種々の伝送手段により受信側に伝送される。暗号文の受信側では、それぞれのグループに対応した暗号解読操作２０，２１で暗号文を解読し、原文を得ることができる。

【００５８】本実施例によれば、テストパターンの持つ規則性を手がかりにして、ＫＡなる暗号化方式または、暗号化鍵による暗号化操作１０によるスクランブリングが第三者に解読されても、ＫＢなる暗号化方式または、暗号化鍵を用いた暗号化操作１１によるスクランブリングが解読されるのを防ぐことができる。

【００５９】図１６、図１７にはコンピュータ１０４を遠隔地にある保守センタ１０５から遠隔保守する場合に本発明が適用された実施例が示されている。コンピュータを遠隔保守する際には保守センタ１０５からコンピュータ１０４にプログラムを転送したり、コンピュータ１０４内のデータをコンピュータ１０４から保守センタ１０５へ転送したりする。この際に、コンピュータで扱うデータのうち＄００、＄ＦＦのデータやＮＯＰを表す機械語コードをＫＡなる暗号化方式または、暗号化鍵による暗号化操作１０により暗号化し、それ以外のデータをＫＢなる暗号化方式または、暗号化鍵による暗号化操作１１により暗号化して、暗号文２を得る。得られた暗号文２は無線や有線などの種々の伝送手段により受信側へ伝送される。暗号文２の受信側では、それぞれのグループに対応した暗号解読操作２０，２１で暗号文２を解読し、原文３を得ることができる。

【００６０】図１８は、図１６、図１７に示す実施例における暗号化の具体例である。

【００６１】原文“＄００００ＦＦＦＦ１２３４”（２進数で 0000 0000 0000 0000 11111111 1111 1111 0001 0010 0011 0100）を暗号化鍵“＄ＡＡ”（２進数で 10101010）との８ビットをブロックとしたビットごとの排他的論理和（exclusive or）を採る従来の方法で暗号化すると暗号文“＄ＡＡＡＡ５５５５Ｂ８９Ｅ”（２進数で 1010 1010 1010 1010 0101 0101 0101 0101 1101 1000 1001 1110）が得られる。

【００６２】また、原文“＄ＦＦ”（２進数で 1111 1111）及び、“＄００”（２進数で0000 0000）を暗号化鍵“＄ＡＡ”、それ以外の原文を暗号化鍵“＄９９”（２進数で 1001 1001）との８ビットをブロックとしたビットごとの排他的論理和（exclusive or）を採る本発明の方法で暗号化すると暗号文“＄ＡＡＡＡ５５５５８ＢＡＤ”（２進数で 1010 1010 1010 1010 0101 0101 0101 0101 1000 1011 1010 1101）が得られる。

【００６３】従来の方法では、コンピュータデータ中（原文中）の“＄ＦＦ”及び、“＄００”の出現頻度が高いという知識から暗号文中で出現頻度の高い“＄ＡＡ”、“＄５５”が原文“＄ＦＦ”、“＄００”に対応する暗号であることが判る。従って暗号化鍵は“＄ＡＡ”または“＄５５”のいずれかであることが判る。従って暗号文“＄Ｂ８９Ｅ”に対応する原文は、“＄１２３４”または、“＄８ＤＣＢ”（２進数で 1000 1101 1

100 1011）であると推定できる。

【００６４】しかし、本発明の方法によると、コンピュータデータ中（原文中）の“＄ＦＦ”及び、“＄００”の出現頻度が高いという知識から暗号文中で出現頻度の高い“＄ＡＡ”、“＄５５”が原文“＄ＦＦ”、“＄００”に対応する暗号であることが判り、暗号化鍵は“＄ＡＡ”または“＄５５”のいずれかであることが判っても暗号文“＄８ＢＡＤ”はまったく異なる暗号化鍵で暗号化されているために、上記の知識から原文を推定することはできない。

【００６５】本実施例によれば、コンピュータデータの出現度数分布を手がかりにして、ＫＡなる暗号化方式または、暗号化鍵を用いた暗号化操作１０による暗号文が第三者に解読されても、ＫＢなる暗号化方式または、暗号化鍵を用いた暗号化操作１１による暗号文が解読されるのを防ぐことができる。

【００６６】図１９、図２０にはＩＤカードやキャッシュカードに本発明が適用された実施例が示されている。これらのカード１０６の磁気記録部分１０７にはＩＤ番号、口座番号とともに正当な使用者であることを認証するために、暗証番号が記録されている場合が多い。この場合、ＩＤ番号、口座番号（原文）１をＫＡなる暗号化方式または、暗号化鍵による暗号化操作１０により暗号化し、暗証番号をＫＢなる暗号化方式または、暗号化鍵を用いた暗号化操作１１により暗号化して、暗号文２を得る。得られた暗号文２は磁気記録手段などによりカード１０６に記録される。カード読み取り機では、それぞれのグループに対応した暗号解読操作２０，２１で暗号文２を解読し、原文３を得て、正当な使用者であるかどうかを判断する。

【００６７】本実施例によれば、カード１０６表面に記載されているＩＤ番号、口座番号を手がかりにして、ＫＡなる暗号化方式または、暗号化鍵を用いた暗号化操作１０による暗号文が第三者に解読されても、暗証番号のＫＢなる暗号化方式または、暗号化鍵を用いた暗号化操作１１による暗号文が解読されるのを防ぐことができる。

【００６８】また暗号化しないまでも、一般に公開されているコード体系、記録方式を用いる場合でも、ＩＤ番号、口座番号と暗証番号を別個のコード体系、記録方式により記録すれば、同様の効果が得られる。例えば、ＩＤ番号、口座番号をアスキーコードで記録し、暗証番号を二進化十進（ＢＣＤ）コードで記録する方法とか、ＩＤ番号、口座番号と暗証番号を異なるアジマス角で記録するなどの方法が考えられる。

【００６９】以上本発明の実施例について説明したが、本発明を従来の暗号化方式と組み合わせて用いると更に暗号強度が増すことはもちろんのことである。例えば、本発明による暗号化を実施したのちにＤＥＳ暗号による暗号化を施せば、コンピュータデータ伝送に最適な暗号化によるデータ伝送方式を提供することができる。

【００７０】

【発明の効果】本発明によれば、原文を構成する文字、符号、データの種別に応じて複数の暗号化方式または暗号化鍵を使い分けるようにしたので、原文中の符号の出現頻度に関する知識や、原文の推定を手がかりにして、暗号が第三者に解読される畏れを少なくすることができる。

【図面の簡単な説明】

【図１】本発明に係る暗号化データの伝送方法の基本的原理を示す説明図である。

【図２】本発明に係る暗号化データの伝送方法の一実施例を示す説明図である。

【図３】本発明に係る暗号化データの伝送方法の一実施例を示す説明図である。

【図４】図３におけるグループ判別手段の具体的構成を示すブロック図である。

【図５】本発明に係る暗号化データの伝送方法の他の実施例を示す説明図である。

【図６】本発明に係る暗号化データの伝送方法の他の実施例を示す説明図である。

【図７】データの暗号化の具体例を示す説明図である。

【図８】図６におけるグループの判別手段４０Ａの具体的構成を示す説明図である。

【図９】図６におけるグループ判別手段４０Ｂの具体的構成を示す説明図である。

【図１０】暗号化鍵が固定パターンでない場合における暗号化の過程を示す説明図である。

【図１１】暗号化鍵が固定パターンでない場合における暗号化の過程を示す説明図である。

【図１２】本発明が適用されるリモートセンシングシステムを概念的に示す説明図である。

【図１３】本発明が適用されるリモートセンシングステムにおける暗号化データの伝送方法の実施例を示す説明図である。

【図１４】本発明が適用される加入放送システムを概念的に示す説明図である。

【図１５】本発明が適用される加入放送システムにおける暗号化データの伝送方法の実施例を示す説明図である。

【図１６】本発明が適用されるコンピュータの遠隔保守システムを概念的に示した説明図である。

【図１７】本発明が適用されるコンピュータの遠隔保守システムにおける暗号化データの伝送方法の実施例を示す説明図である。

【図１８】図１７におけるデータの暗号化の具体例を示す説明図である。

【図１９】本発明が適用されるＩＤカードの外観を示す説明図である。

【図２０】本発明が適用されるＩＤカードを用いた暗号

15　　16

化データの伝送方法の実施例を示す説明図である。

【符号の説明】

１，３　原文

２　暗号文

１０～１２　暗号化操作

２０～２２　暗号解読操作

３０～３３　スイッチ

４０，４０Ａ，４０Ｂ　グループ判別手段

＊４３－１～４３－Ｎ　比較器群

４５－１～４５－Ｎ　比較器群

４７－１～４７－Ｎ　比較器群

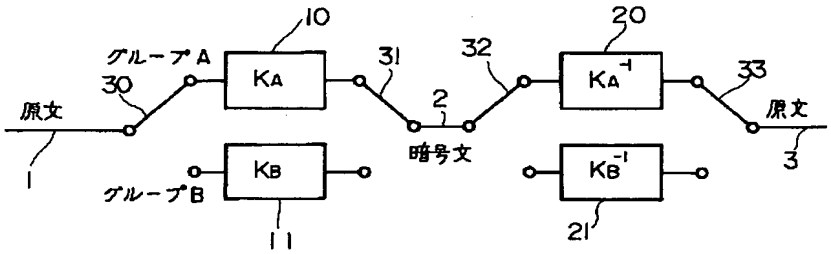
４９－１～４９－Ｎ　比較器群

５０－１，５０－２　オアゲート

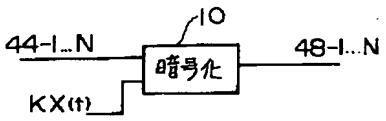
６０－１，６０－２　オアゲート

５１，６１　アンドゲート

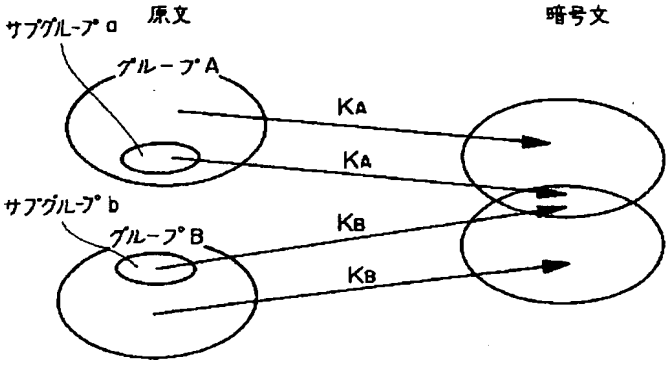
【図１】



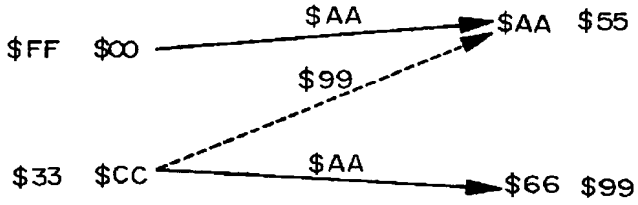
【図１１】



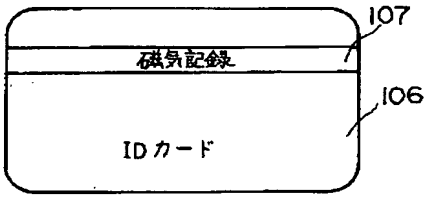
【図２】



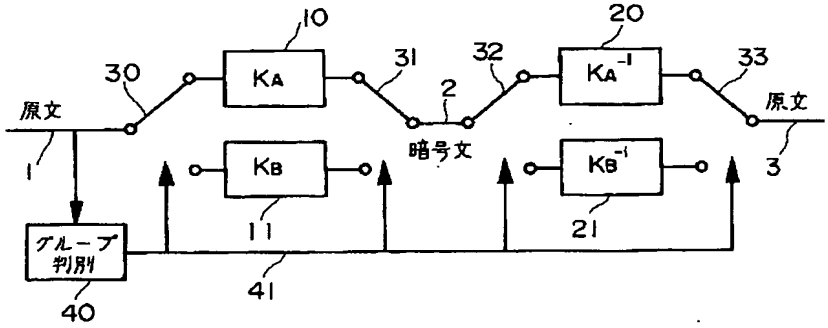
【図７】



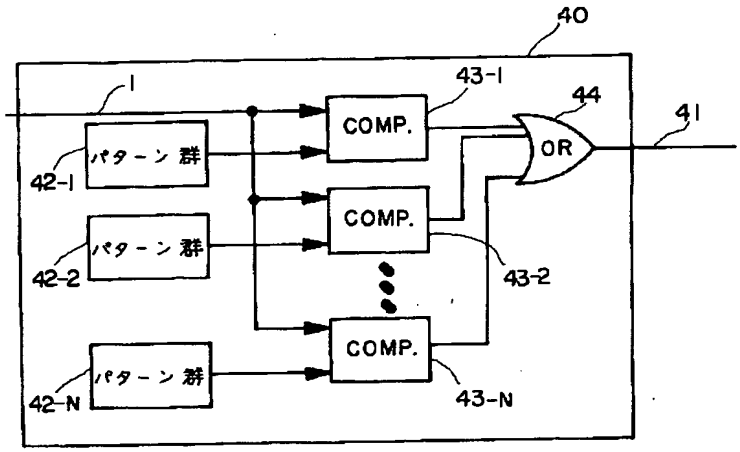
【図１９】



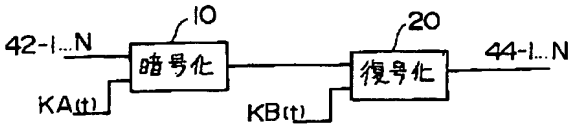
【図３】



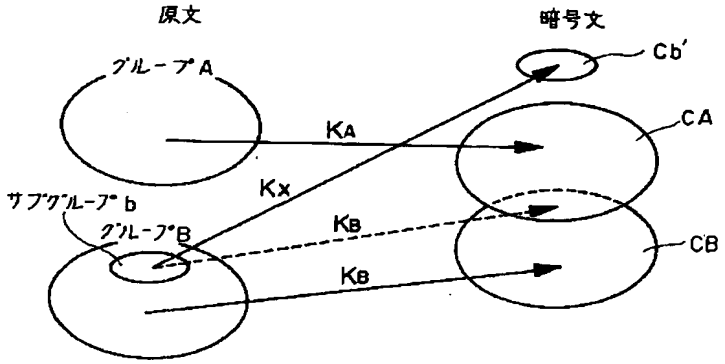
【図４】



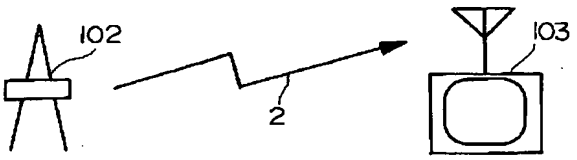
【図１０】



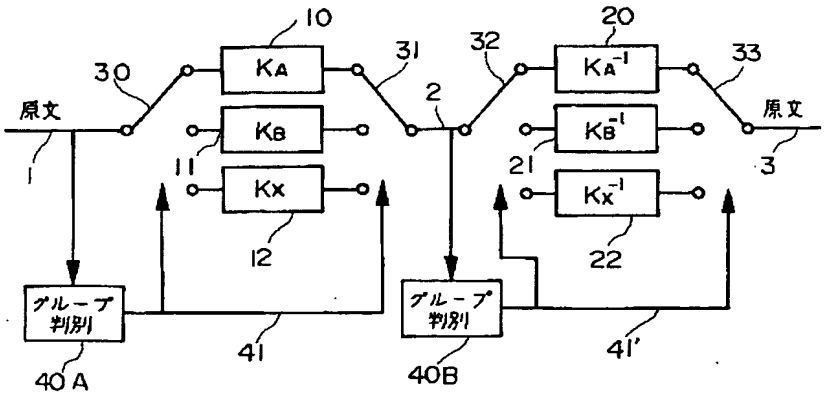
【図５】



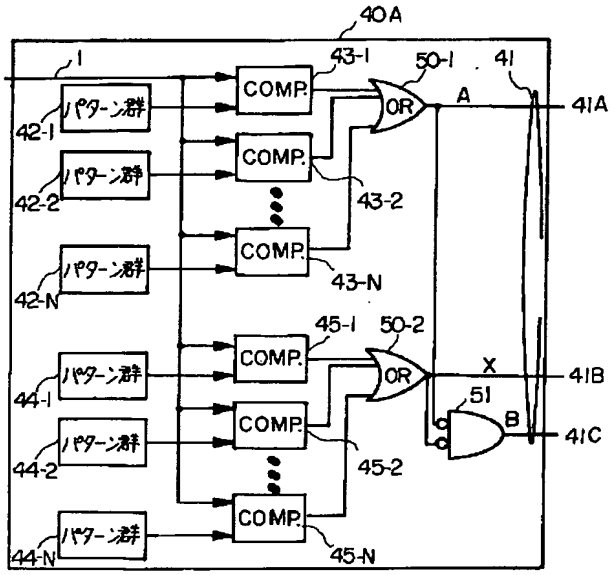
【図１４】



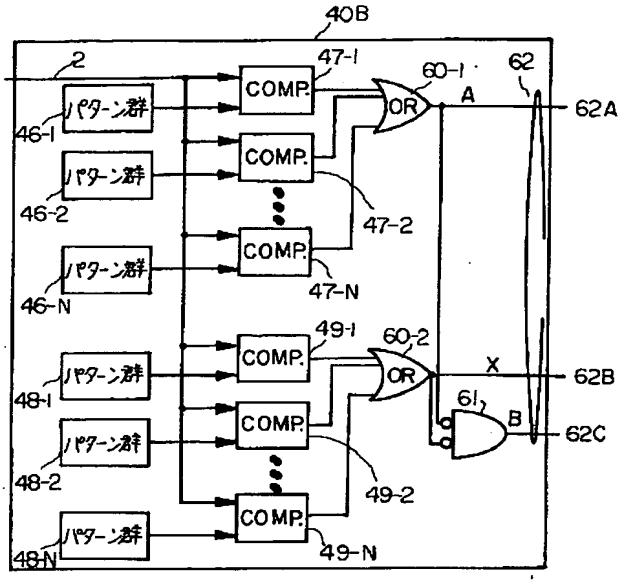
【図６】



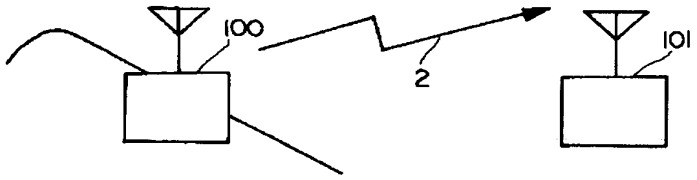
【図8】



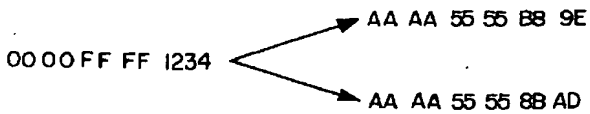
【図9】



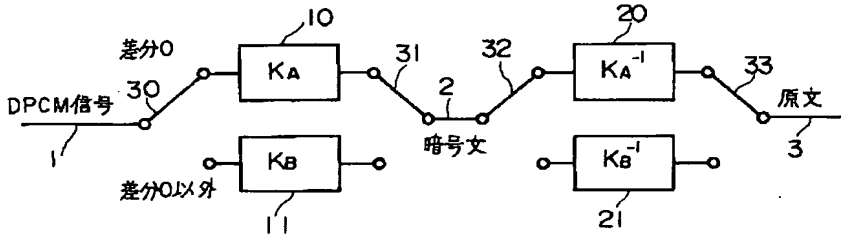
【図12】



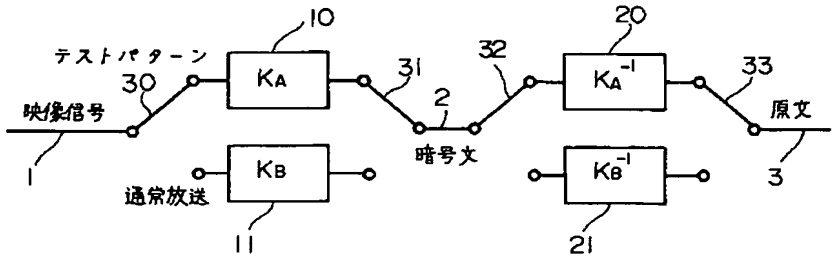
【図18】



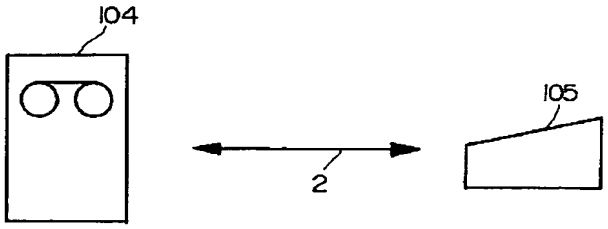
【図13】



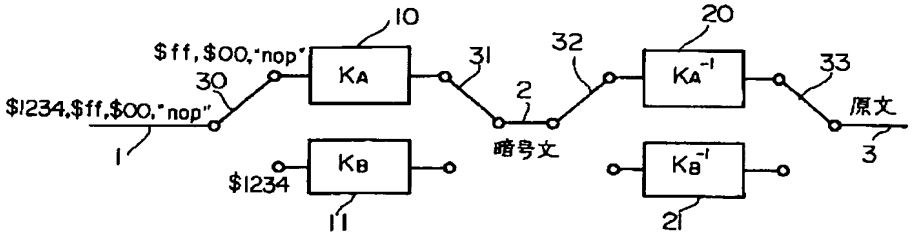
【図１５】



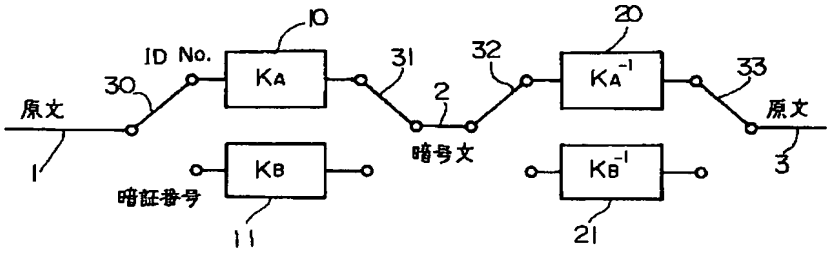
【図１６】



【図１７】



【図２０】



フロントページの続き

(51)Int.Cl.[5]	識別記号	庁内整理番号	FI	技術表示箇所
Ｇ０９Ｃ 1/00		9194－5L		
Ｈ０４Ｋ 1/00		Z 7117－5K		